Los expertos han emitido una advertencia sobre una nueva y avanzada forma de estafa telefónica por voz (vishing) conocida como *«Letscall»*. Este método está dirigido actualmente a personas en Corea del Sur.

Los delincuentes detrás de *Letscall* emplean un ataque en varias etapas para engañar a las víctimas y hacer que descarguen aplicaciones maliciosas desde un sitio web falsificado de Google Play Store.

Una vez que el software malicioso se instala, redirige las llamadas entrantes a un centro de llamadas controlado por los criminales. Operadores capacitados que se hacen pasar por empleados bancarios extraen información confidencial de personas desprevenidas.

Para facilitar el enrutamiento del tráfico de voz, Letscall utiliza tecnologías avanzadas como voz por IP (VoIP) y WebRTC. También aprovecha los protocolos de Traversal de Sesiones para NAT (STUN) y Traversal Utilizando Relés alrededor de NAT (TURN), incluyendo servidores STUN de Google, para garantizar llamadas telefónicas o de video de alta calidad y sortear las restricciones de NAT y firewall.

El grupo Letscall está compuesto por desarrolladores de Android, diseñadores, programadores de front-end y back-end, así como operadores telefónicos especializados en ataques de ingeniería social por voz.

El malware opera en tres fases: en primer lugar, una aplicación de descarga prepara el dispositivo de la víctima, allanando el camino para la instalación de un software espía potente. Este software espía luego desencadena la etapa final, que permite redirigir las llamadas entrantes al centro de llamadas controlado por los atacantes.

> *«La tercera fase cuenta con un conjunto de comandos propio, que incluye también comandos de WebSocket. Algunos de estos comandos están relacionados con la manipulación de la agenda de contactos, como crear y eliminar contactos. Otros comandos se refieren a la creación, modificación y eliminación de filtros que*

> *determinan qué llamadas deben ser interceptadas y cuáles deben ser ignoradas»,* señaló la empresa holandesa de seguridad móvil ThreatFabric en su informe.

Lo que distingue a Letscall es su utilización de técnicas de evasión avanzadas. El malware incorpora técnicas de ofuscación como Tencent Legu y Bangcle (SecShell) durante la descarga inicial. En etapas posteriores, utiliza estructuras de nombres complejas en los directorios de archivos ZIP y corrompe intencionalmente el manifiesto para confundir y evadir los sistemas de seguridad.

Los delincuentes han desarrollado sistemas que llaman automáticamente a las víctimas y reproducen mensajes previamente grabados para engañarlas aún más. Mediante la combinación de infecciones en teléfonos móviles con técnicas de estafa telefónica (vishing), estos estafadores pueden solicitar micropréstamos utilizando los nombres de las víctimas, al mismo tiempo que les aseguran actividades sospechosas y redirigen las llamadas a sus propios centros.

Las consecuencias de este tipo de ataques pueden ser significativas, dejando a las víctimas cargadas con préstamos considerables por pagar. Con frecuencia, las instituciones financieras subestiman la gravedad de estas invasiones y no investigan posibles fraudes.

Aunque esta amenaza se encuentra actualmente limitada a Corea del Sur, los investigadores advierten que no existen barreras técnicas que impidan que estos atacantes se expandan a otras regiones, incluyendo la Unión Europea.

Esta nueva forma de ataque de suplantación de identidad por voz resalta la constante evolución de las tácticas delictivas y su capacidad para aprovechar la tecnología con fines maliciosos. El grupo responsable del malware conocido como Letscall muestra un conocimiento detallado de la seguridad de Android y de las tecnologías de enrutamiento de

voz.